



| Brief |

The Underground Economist: Volume 4, Issue 6

B-2024-03-14a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Vulnerability Exploitation, Deep and Dark Web,
Social Media

March 14, 2024

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 9:00 AM (EDT) on March 14, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | The Underground Economist: Volume 4, Issue 6

| Threat Actors Continue to Exploit ZeroLogon Vulnerability

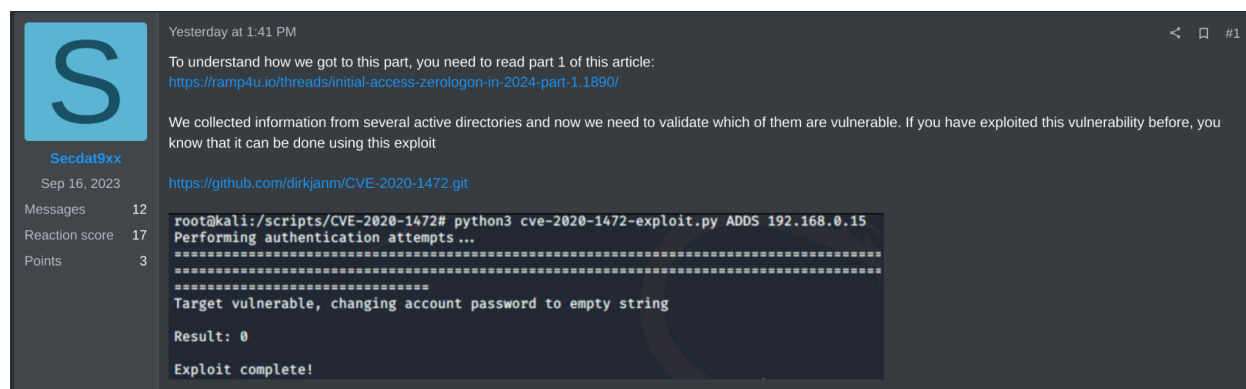
Nearly four years after its discovery, CVE-2020-1472 (ZeroLogon) is almost certainly still being exploited by malicious actors. On March 10, 2024, well-regarded English-speaking threat actor “Secdat9xx” posted in deep and dark web (DDW) community RAMP a detailed, two-part manual covering how the ZeroLogon vulnerability can still be exploited.

- ZeroLogon is a privilege-elevation vulnerability with a NIST severity score of 10.0 (critical). Successfully exploited, it enables threat actors to establish a vulnerable Netlogon secure channel connection to a domain controller using the Netlogon Remote Protocol (MS-NRPC). This can enable the attacker to gain domain administrator access.¹

The first part of the manual covers scanning for potentially vulnerable servers via Censys to collect their IPs. Then, coder “dirkjanm”’s 2020 proof-of-concept (PoC) for ZeroLogon and the CrackMapExec network pentesting tool, both readily available on GitHub, are deployed to identify the vulnerable servers from the IP list generated via Censys. A Metasploit module is then deployed to remove an administrator’s password. Utilizing

¹ [hXXps://nvd.nist\[.\]gov/vuln/detail/cve-2020-1472](https://nvd.nist.gov/vuln/detail/cve-2020-1472)

these steps, Secdat9xx was able to access the active directory of the entity at innotech-sa[.]com (a technological company based in Saudi Arabia) via the pass-the-hash technique.



RAMP post by Secdat9xx introducing exploitation instructions

Source: ZeroFox Intelligence

- The actor's peers on RAMP reacted positively to the manual, and some of them will likely be prompted to implement or repost it.
- The finding indicates that a sufficient number of networks remain vulnerable to warrant a threat actor leveraging the ZeroLogon attack flow. This reinforces the often-made observation that many successful cyberattacks occur via the leveraging of well-developed exploits and attack flows against networks that remain vulnerable a significant length of time following the vulnerabilities initial identification and remediation.

| X Account Sales in DDW Forums Continue to Diversify

On March 8, 2024, positive-reputation Russian-speaking threat actor "investimer" announced in DDW forum exploit[.]in that they are selling X accounts that include either USD 500 or EUR 500, which can be spent on promotional ads. The accounts, which are advertised for USD 50 each, also include details for an associated payment method.

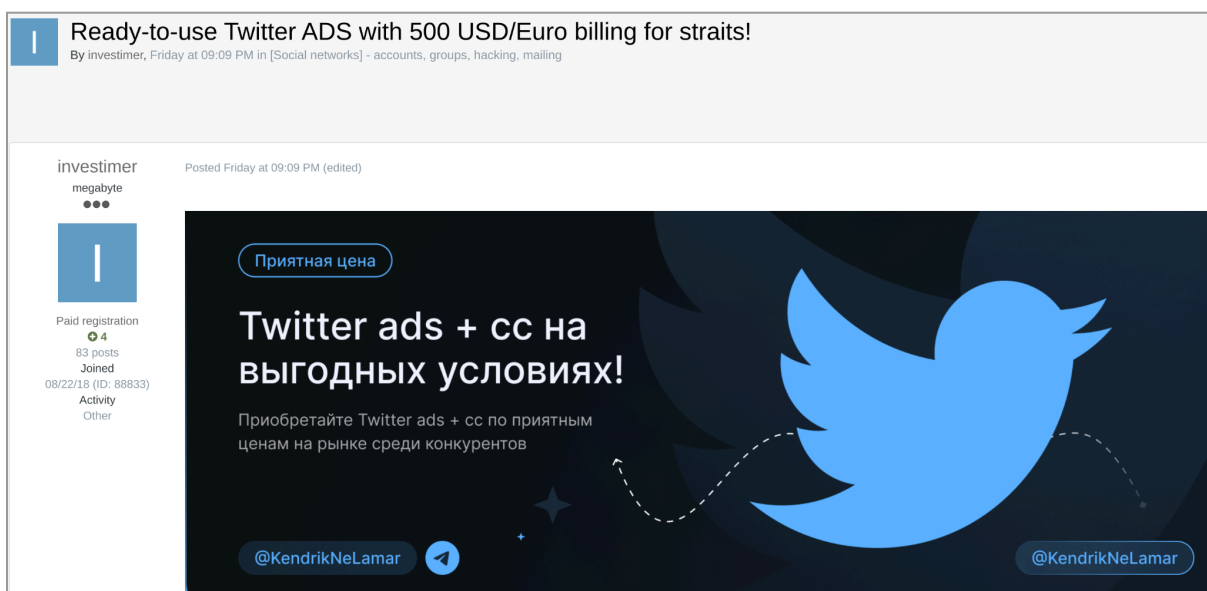
- As of Q1 2024, eligible X business accounts may purchase ads, which are used to publicly promote their content. As of the writing of this report, it is not clear how

malicious users spend this advertising credit. However, this is very likely to appeal to politically or ideologically-motivated threat actors seeking to influence opinion, as well as to those able to leverage malicious advertisements in the conducting of social engineering campaigns.

- The inclusion of payment information indicates it is likely the USD/EUR 500 credit has been funded by personal data, which along with the accounts themselves, has been stolen.

The actor's Telegram channel, Kendrik Shop, allows buyers to make automated purchases without interaction with the seller. At the time of writing, 10 accounts were for sale in the shop and can be purchased via several types of cryptocurrencies—including Bitcoin (BTC), Ethereum (ETH), or Tether (USTD)—offering anonymity for the buyer.

ZeroFox has observed several new services specializing in the sale of illicitly-obtained social media accounts in 2024, indicating a very likely chance that they are growing in popularity. X accounts are almost certainly in the highest demand; this is very likely due in part to low levels of moderation, high levels of inherent anonymity, and the ability of threat actors to leverage licit as-a-service tools to bypass Know Your Customer (KYC) protocols, which are often associated with the creation of social media accounts.



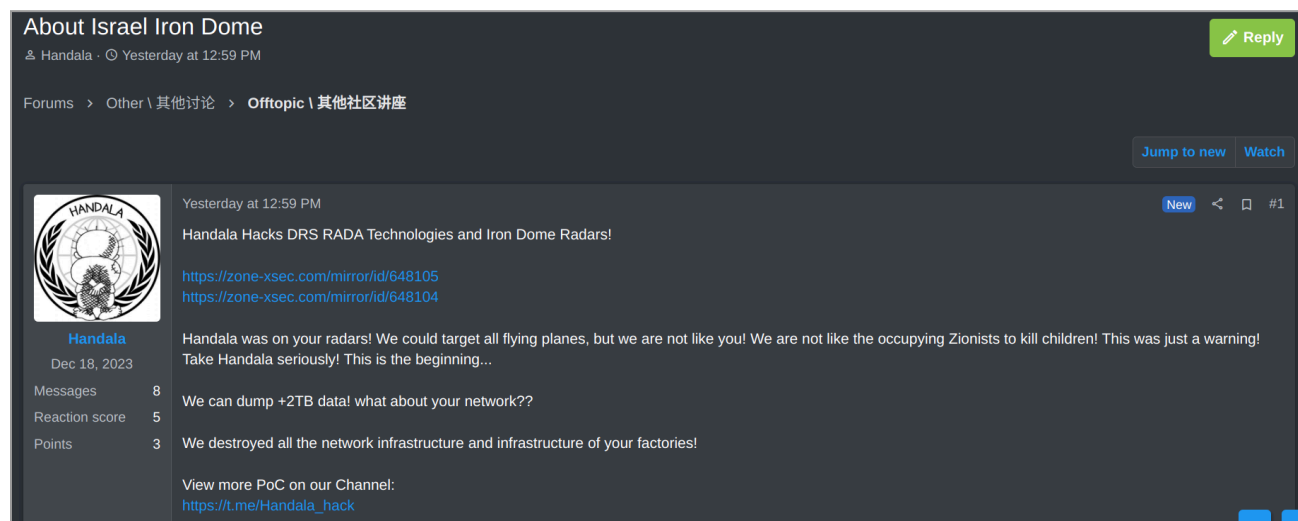
Post by investimer advertising X accounts for sale

Source: ZeroFox Intelligence

Threat Actors Target Israel over Possible Rafah Incursion

On March 3, 2024, hacktivist organization Handala boasted of successfully infiltrating the servers of DRS Rada Technologies (RADA), an Israeli defense company that manufactures radar solutions and legacy avionics systems, on dark web forum RAMP. The group also claimed an attack against Israel's Iron Dome infrastructure.

- The latter is more high profile, as the Iron Dome is a well-known anti-missile technology that Israel has used to down projectiles fired from Gaza.
- However, the targeting of radar technologies could be more impactful as Israel currently utilizes its air force more frequently than the Iron Dome, which was primarily used at the onset of the war when Hamas was able to maintain constant rocket attacks on Israel.
- ZeroFox notes that previous claimed attacks against the Iron Dome, most recently by self-styled hacktivist organizations Anonymous Sudan in May 2023 and Anonymous Arabia in January 2024, appear to have had little impact on the system.²³



Handala's claim of hacking RADA

Source: ZeroFox Intelligence

² [hXXps://www.jpost\[.\]com/israel-news/article-741869](https://www.jpost.com/israel-news/article-741869)

³ [hXXps://tgstat\[.\]com/channel/@Anonymous_v7X/62](https://tgstat[.]com/channel/@Anonymous_v7X/62)

Handala claimed that it could have targeted “all flying planes” but did not do so since the group is not “like the occupying Zionists” who “kill children.”

- While it is highly unlikely the group could have downed Israeli aircraft, Handala did claim to have taken down RADA’s factory data, and the company’s website remains down.
- A prolonged outage could impact Israel’s ability to carry out its military operations. If the leaked radar output and stolen technical information were disclosed to Israel’s regional enemies, such as Iran, it could put Israeli forces at a disadvantage against Tehran’s proxies—particularly in the case of a significant escalation with Hezbollah, which is thought to possess up to 150,000 rockets and missiles that could be used against air and ground targets.

In addition to live radar interface instances, the actor also claimed to have accessed RADA’s factories. Allegedly, 2 terabytes of data were stolen and can be disclosed to the DDW public. Handala left its TOX contact, indicating the group expected representatives of RADA to contact them and negotiate regarding the stolen data.

- No ransom value was stated, indicating the group has political rather than financial motives.

The websites drsrada[.]com and rada[.]co[.]il were also defaced with messages threatening more attacks if Israel continues with its offensive in Rafah.

Defacement Details of <https://rada.co.il>

Saved on: 2024-03-03 17:42:11 Defacer: handala hack team Location: 
IP: 104.21.10.11 Team: handala hack team Web Server: Cloudflare Server

 image

Hacked By Handala Hack Team

We stood by Rafah! This was just a warning...

Free Palestine

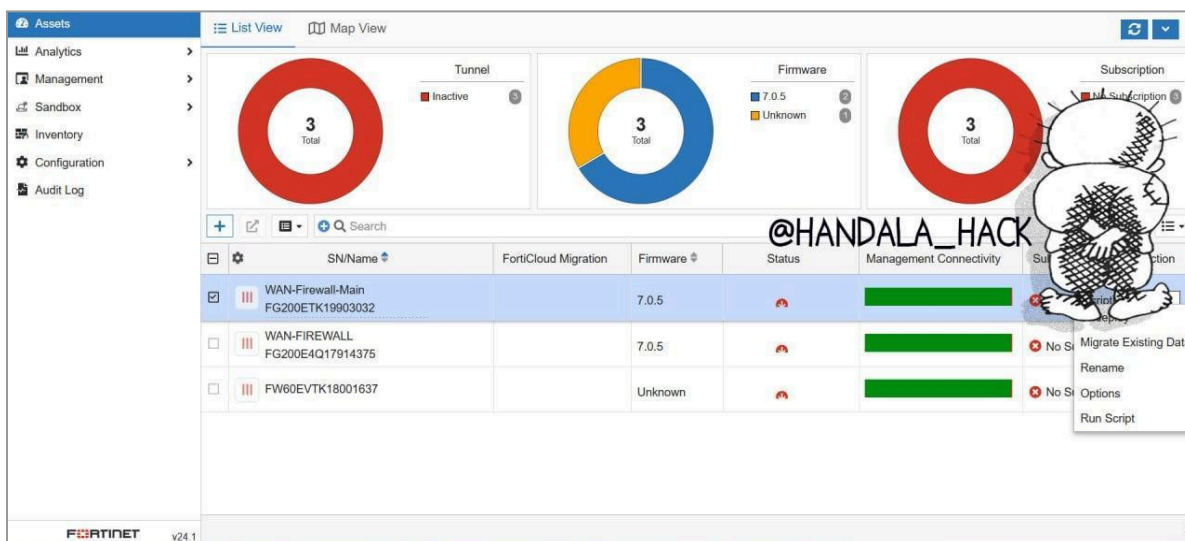
As long as the bullets and bloodshed in my land do not get tired and the wound is still on the leg, we will stand.

Telegram: @Handala_hack
www.handala.cx

Defacement message on [drsrada\[.\]com](https://drsrada[.]com) and [rada\[.\]co\[.\]il](https://rada[.]co[.]il)

Source: ZeroFox Intelligence

- Handala also has a website “under construction” at [handala\[.\]cx](http://handala[.]cx), indicating that the team plans on expanding its activities.



Website “under construction” at [handala\[.\]cx](http://handala[.]cx)

Source: ZeroFox Intelligence

This development comes against a backdrop of intensive ceasefire negotiations and Israeli threats to invade the southern Gazan city of Rafah during Ramadan (March 10–April 9, 2024). According to numerous reports, Israeli officials have agreed to the “framework” of a deal that would see a six-week ceasefire, including the release of an unspecified number of hostages held by Palestinian militants in the Gaza Strip.⁴ However, the agreement hit a snag when Hamas failed to provide a list of living hostages, claiming that gathering such information is impossible in an active war zone. Disagreements also reportedly remain regarding the right of Palestinian citizens to reoccupy their homes in areas declared “cleared” by Israeli forces.⁵

The international community, and especially the United States, has continued to push for a deal to ease the humanitarian crisis in the enclave, which became more pressing following the Al-Rashid incident in which over 100 Palestinian civilians were killed while attempting to get food from aid trucks on February 29, 2024.⁶

The failure to secure a ceasefire and further humanitarian issues triggered by a subsequent invasion of Rafah, which currently houses hundreds of thousands of refugees, would likely incentivize pro-Palestinian actors to increase cyberattacks against Israeli targets and interests.

⁴

[hXXps://www.timesofisrael\[.\]com/us-says-israel-has-agreed-to-framework-for-gaza-truce-ball-is-in-hamass-court/](https://www.timesofisrael.com/us-says-israel-has-agreed-to-framework-for-gaza-truce-ball-is-in-hamass-court/)

⁵ [hXXps://www.jpost\[.\]com/breaking-news/article-789931](https://www.jpost.com/breaking-news/article-789931)

⁶ [hXXps://news.sky\[.\]com/story/what-we-know-so-far-about-deadly-aid-truck-incident-in-gaza-city-13083952](https://news.sky.com/story/what-we-know-so-far-about-deadly-aid-truck-incident-in-gaza-city-13083952)

| Recommendations

- Adopt a Zero-Trust cybersecurity architecture based upon a principle of least privilege.
- Implement network segmentation to separate resources by sensitivity and/or function.
- Implement secure password policies with phishing-resistant multi-factor authentication (MFA), complex passwords, and unique credentials.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated tactics, techniques, and procedures (TTPs).
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud servers at least once per year—and ideally more frequently.
- Develop a comprehensive incident response strategy.
- Configure email servers to block emails with malicious indicators and deploy authentication protocols to prevent spoofed emails.
- Deploy a holistic patch management process and ensure all IT assets are updated with the latest software updates as quickly as possible.
- Proactively monitor for compromised accounts being brokered in deep and dark web forums.
- Configure ongoing monitoring for Compromised Account Credentials.

| Appendix A: Traffic Light Protocol for Information Dissemination

WHEN SHOULD IT BE USED?

Red

Sources may use

TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.

Amber

Sources may use

TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.

HOW MAY IT BE SHARED?

Recipients may NOT share

TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.

Recipients may ONLY share

TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.

Note that

TLP:AMBER+STRICT restricts sharing to the organization only.

Green

WHEN SHOULD IT BE USED?

Sources may use

TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.

Clear

Sources may use

TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.

HOW MAY IT BE SHARED?

Recipients may share

TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.

Recipients may share

TLP:CLEAR information without restriction, subject to copyright controls.

| Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%